

(12)

DEMANDE DE BREVET D'INVENTION

A1

(22) Date de dépôt : 09.10.92.

(30) Priorité :

(43) Date de la mise à disposition du public de la demande : 15.04.94 Bulletin 94/15.

(56) Liste des documents cités dans le rapport de recherche préliminaire : Se reporter à la fin du présent fascicule.

(60) Références à d'autres documents nationaux apparentés :

(71) Demandeur(s) : KUDELSKI (S.A.) FABRIQUE D'ENREGISTREURS NAGRA — CH.

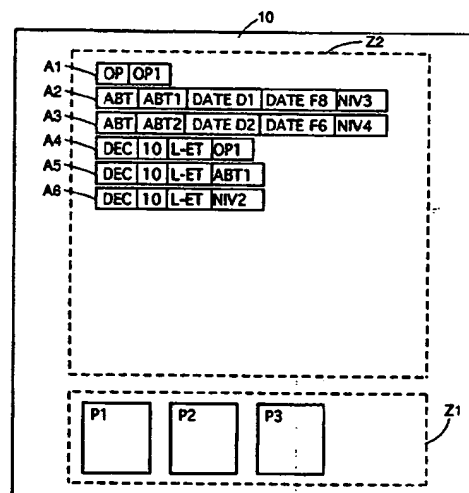
(72) Inventeur(s) : Kudelski André.

(73) Titulaire(s) :

(74) Mandataire : Moinas Michel.

(54) Système de traitement d'information utilisant un ensemble de cartes à mémoire.

(57) Système de traitement d'information comprenant un ensemble de cartes à mémoire et au moins une unité centrale de gestion. Selon l'invention, les cartes à mémoire et l'unité centrale de gestion constituent ensemble une base de données relationnelle. Chaque carte à mémoire contient une mémoire destinée à stocker un ensemble d'instructions (A1, A2,..., An), chaque instruction contenant un lien logique avec au moins une autre instruction.



FR 2 696 854 - A1



SYSTÈME DE TRAITEMENT D'INFORMATION UTILISANT UN ENSEMBLE DE CARTES À MÉMOIRE

La présente invention concerne de façon générale un système de traitement d'information, ce système comprenant un ensemble de cartes à mémoire et au moins une unité centrale de gestion.

5 On connaît un grand nombre de systèmes de traitement d'information comprenant un ensemble de cartes à mémoire et au moins une unité centrale de gestion. Dans ces systèmes connus, on trouve des cartes à mémoire (parfois appelées cartes à puce) qui sont habituellement des cartes incluant chacune au moins un
10 circuit intégré constituant un micro-contrôleur comprenant des mémoires de type ROM, RAM, EPROM et/ou EEPROM dont l'accès est contrôlé par un logiciel intégré. Dans ces systèmes connus, on trouve aussi au moins une unité centrale de gestion qui est extérieure aux cartes à puce et qui dispose d'un droit sur au
15 moins une zone de certaines cartes à puce ou de toutes les cartes à puce.

Dans la suite du texte on appellera aussi "opérateur" une telle unité centrale de gestion. D'autre part, on appellera "émetteur" un tel opérateur disposant du droit d'allouer des
20 zones opérateur sur les cartes à mémoire.

Depuis que la carte à mémoire a vu le jour, un certain nombre d'applications utilisant cette technologie sont apparues.

Une première génération connue de cartes à mémoire faisait intervenir un opérateur capable de "conserver" les
25 secrets qui étaient contenus dans la carte et un certain nombre d'opérateurs pouvaient consulter les informations non-critiques.

Une seconde génération connue de cartes à mémoire, principalement utilisée dans le domaine de la télévision à péage, prévoit pour chaque carte un nombre variable d'opérateurs

pouvant disposer librement et exclusivement de leurs zones privées. Parmi les opérateurs, on trouve l'émetteur de télévision qui est capable de créer de nouveaux opérateurs.

5 Cette structure de carte à mémoire rend hermétique toute communication entre les zones des différents opérateurs, de façon à assurer la sécurité du système. Ainsi, l'émetteur n'aura en principe pas de droit d'accès à une zone concédée à un opérateur distinct.

10 Pour chaque nouveau prestataire de services, il sera nécessaire d'ouvrir une nouvelle zone sur la carte.

Afin d'illustrer une telle situation, on peut considérer la situation suivante (volontairement simplifiée).

15 En admettant qu'un abonné de télévision à péage X désire souscrire à trois chaînes de télévision A, B et C, il devra prendre contact avec chacune de ces chaînes qui feront inscrire (par le signal d'antenne) les ordres d'ouverture de zones respectives dans la carte de l'abonné. La carte de l'abonné X disposera de 4 zones ouvertes sur la carte, à savoir la zone "émetteur" et les trois zones des chaînes A, B et C. L'ouverture des zones sera
20 effectuée par l'émetteur qui est seul à disposer du droit d'ouvrir de nouvelles zones, ou plus précisément du droit de gérer les ressources globales de la carte. Ce principe de gestion est actuellement utilisé dans la norme Eurocrypt de télévision à péage.

25 Ces cartes de deuxième génération connues présentent les limitations suivantes.

Du fait de la mise en place plusieurs systèmes de télévision à péage et de distribution d'informations, il se produit les limitations suivantes :

30 A. Les systèmes connus sont calqués sur les systèmes informatiques classiques, à savoir le découpage d'une partie de mémoire en plusieurs zones, chacune étant réservée à son utilisateur. Parallèlement, on considère que l'opérateur (prestataire de service) accède de façon identique à chacune des

cartes, à l'instar de l'utilisateur d'un ordinateur qui se connecte avec son mot de passe sur sa machine.

5 B. Les modèles de gestion retenus sont calqués sur les possibilités antérieures à la messagerie électronique. Le modèle n'a pas été revu en fonction des nouvelles possibilités offertes par un flux d'informations entre un émetteur et chaque carte à mémoire.

10 C. Les structures de distribution des informations se trouvent en réalité beaucoup plus complexes que les modèles prévus à l'origine, compliquant et limitant passablement les possibilités de gestion.

15 D. Le fait d'avoir, en télévision à péage, un flux principalement unidirectionnel entre l'opérateur et la carte à mémoire, où l'on ne peut jamais être sûr que le message a bien été reçu, pose des difficultés opérationnelles difficiles à modéliser.

20 Un objet de l'invention consiste à proposer un nouveau système de traitement d'information, ce système comprenant un ensemble de cartes à mémoire et au moins une unité centrale de gestion, dans lequel la gestion des informations contenues dans les cartes à mémoire est facilitée.

Un autre objet de l'invention consiste à proposer un tel système dans lequel une modification du nombre des unités centrales de gestion peut être traitée plus facilement.

25 Un autre objet de l'invention consiste à proposer un tel système dans lequel une modification du type de unité centrale de gestion peut être traitée plus facilement.

30 Un autre objet de l'invention consiste à proposer un tel système dans lequel une modification de la hiérarchie de certains droits ou de certaines obligations liées à plusieurs unités centrales de gestion peut être traitée plus facilement.

L'invention concerne donc un système de traitement d'information comprenant un ensemble de cartes à mémoire et au moins une unité centrale de gestion.

Selon une caractéristique essentielle de l'invention, les cartes à mémoire et l'unité centrale de gestion constituent ensemble une base de données relationnelle.

5 Selon une mode de réalisation particulier de l'invention, chaque carte à mémoire contient une mémoire destinée à stocker un ensemble d'instructions (A1, A2,... , An), chaque instruction contenant un lien logique avec au moins une autre instruction.

10 Selon une autre mode de réalisation particulier de l'invention, chaque carte à mémoire contient en outre au moins un programme spécifique (P1) qui est destiné à exécuter une fonction spécifique de la carte à mémoire en appliquant les liens logiques qui sont instaurés entre les différentes instructions contenues dans la carte à mémoire.

15 L'invention concerne aussi un ensemble de cartes à mémoire.

Selon une mode de réalisation particulier de l'invention, chaque carte à mémoire de l'ensemble comprend des informations d'une base de données relationnelle et en ce que l'ensemble des informations dudit ensemble de cartes à mémoire
20 constitue une mémoire de stockage d'une base de données relationnelle.

Autrement dit, un nouveau système est proposé, ce système étant défini comme une structure où les informations ne sont pas stockées dans des cases prédéfinies, en vue de leur
25 utilisation, mais où les informations sont mémorisées en fonction de la place disponible dans la mémoire et voient leur rôle déterminé par les conditions d'utilisation associées.

Ces objets, caractéristiques et avantages, ainsi que d'autres, seront mieux compris lors de la description détaillée
30 qui va suivre d'un mode de réalisation donné seulement à titre d'exemple non limitatif, illustré par les figures annexées parmi lesquelles :

la figure 1 illustre un système selon la présente invention ;

la figure 2 est un diagramme montrant le mode de stockage d'informations dans une carte à mémoire du système selon l'invention ;

la figure 3 représente un exemple d'une configuration
5 générale de diffusion de plusieurs chaînes de télévision ; et

la figure 4 représente de façon simplifiée la structure d'une carte à mémoire d'un système selon la présente invention.

Sur la figure 1, on voit de façon schématique un exemple
d'un système selon l'invention. Ce système est constitué par un
10 certain nombre de cartes à mémoire 10, un réseau de communication de données 12, au moins une unité centrale de gestion, appelée "opérateur", 14 (ici deux opérateurs sont représentés), connectés au réseau 12, et au moins un dispositif de connexion de carte 16 (ici quatre sont représentés) connectés
15 au réseau 12. A tout moment, une carte peut être reliée aux opérateurs 14 en étant connectée à un des dispositifs de connexion 16. Cette configuration correspond par exemple à un système de cartes bancaires. Dans le cas de la télévision à péage, les opérateurs 14 sont des émetteurs de télévision ou des
20 agences offrant certains services commerciaux liés à la télévision à péage (gestion des abonnements, etc ...), le réseau 12 n'est pas une ligne physique mais est constitué par la propagation hertzienne ou par câble du signal vidéo, les dispositifs de connexion 16 sont des décodeurs d'abonnés et les
25 cartes 10 sont des cartes à mémoire, un abonné possédant un décodeur 16 et une carte 10 connectable au décodeur afin de pouvoir recevoir une émission décodée ou débrouillée. Le système selon l'invention peut donc s'appliquer dans deux grandes familles, une famille du type réseau bancaire et une
30 famille du type télévision à péage. La différence entre ces deux familles réside principalement dans le fait que dans un réseau bancaire des informations peuvent passer dans les deux sens entre l'opérateur et la carte alors que dans une télévision à péage l'information passe essentiellement dans le sens
35 opérateur (émission) vers carte (réception).

Sur la figure 2, on voit un certain nombre de cases qui représentent schématiquement des informations qui sont stockées dans une mémoire vive, par exemple une EEPROM, d'une carte à mémoire 10 d'un système selon l'invention qui est appliqué par exemple en télévision à péage.

Quand une carte 10 est connectée à un opérateur 14, la carte reçoit un certain nombre d'informations en provenance de l'opérateur.

La carte contient une zone mémoire Z1 qui contient un certain nombre de programmes spécifiques P1, P2, P3 dont chacun correspond à un mode d'utilisation de la carte. Par exemple, en télévision à péage, la carte peut servir :

- à décoder une émission reçue, (programme P1)
- à acheter des droits sur des émissions à venir, (programme P2)
- à subir une modification du crédit d'émission, (programme P3)
- etc ...

La carte contient aussi une zone mémoire Z2 dont la fonction sera précisée par la suite.

Prenons l'exemple de l'utilisation de la carte 10 pour décoder une émission reçue. L'opérateur envoie une instruction spécifique DEC qui est reçue par la carte qui active alors le programme P1 qui correspond à cette fonction de décodage d'émission reçue DEC. L'opérateur envoie alors un certain nombre d'instructions A1, A2, A3, ... An qui seront stockées dans la zone Z2 de la carte, à la suite les unes des autres, dans l'ordre où elles arrivent. L'ordre de stockage ou l'emplacement du stockage dans la zone Z2 n'a pas d'importance. L'une des originalités du système selon l'invention réside dans le fait que ces instructions A1, A2, A3, ... An sont des "liens logiques entre des données" (que l'on appellera par la suite simplement des "liens") et non de simples données. Par exemple, comme cela est représenté sur la figure 2, on peut trouver les instructions suivantes :

Instruction A1

OP signifie cette instruction concerne une désignation d'opérateur autorisé

OP1 signifie cet opérateur autorisé est l'opérateur N°1

5

Instruction A2 :

ABT signifie cette instruction concerne un droit d'abonnement acquis

ABT1 signifie concerne l'abonnement N° 1

10 DATE D1 signifie date de début 1 de cet abonnement

DATE F8 signifie date de fin 8 de cet abonnement

NIV 3 signifie niveau du droit de réception 3 (par exemple, un niveau 1 peut correspondre aux sports, un niveau 2 aux sports + films, un niveau 3 aux sports + films + variétés, un

15 niveau 4 à toutes émissions, etc...)

Instruction A3 :

ABT signifie cette instruction concerne un droit d'abonnement acquis

20 ABT2 signifie concerne un autre abonnement N° 2

DATE D2 signifie date de début 2 de cet abonnement

DATE F6 signifie date de fin 6 de cet abonnement

NIV 4 signifie niveau du droit de réception 4

25 On peut trouver ensuite d'autre types d'instructions qui sont les suivantes :

Instruction A4

DEC signifie cette instruction concerne un décodage

30 10 signifie lien 10 (c'est-à-dire que toutes les instructions qui ont le même N° de lien sont liées logiquement entre elles)

L-ET lien logique ET (habituellement on trouve des liens logiques ET, OU, NI, etc ...)

35 OP1 l'opérateur qui envoie cette instruction est

l'opérateur N°1

Instruction A5

- DEC signifie cette instruction concerne un décodage
 5 10 signifie lien 10
 L-ET lien logique ET
 ABT1 signifie l'opérateur qui envoie cette instruction
 diffuse un abonnement N°1

10 Instruction A6

- DEC signifie cette instruction concerne un décodage
 10 signifie lien 10
 L-ET lien logique ET
 NIV 2 signifie l'opérateur qui envoie cette instruction
 15 diffuse une émission de niveau 2

Les instructions A1 à A3 sont des droits qui ont été donnés à la carte antérieurement. Autrement dit, à un certain moment, un opérateur autorisé est désigné par opérateur N°1 (instruction A1), puis un opérateur autorisé a inscrit dans (donné à) la carte les droits pour l'abonnement N°1 (instruction A2) et à un autre moment, le même opérateur ou un autre opérateur autorisé a inscrit dans (donné à) la carte les droits pour l'abonnement N°2 (instruction A3).

25 Les instructions A4 à A6 sont des instructions envoyées par un opérateur à la carte en même temps que l'opérateur diffuse une émission brouillée, ces instructions permettant de n'autoriser le débrouillage (ou décodage) par le décodeur auquel est connecté cette carte que si les conditions de droits acquis
 30 par la carte sont satisfaites.

Lors de la réception des instructions A4 à A6, la carte reconnaît que ces instructions concernent une fonction de décodage (code DEC) et par conséquent la carte active son programme spécifique P1 qui sert à n'autoriser le décodage que

si les droits sont acquis. Ce programme spécifique P1 fonctionne en conséquence de la manière suivante :

5 (1) considérer toutes les instructions qui ont un "lien" entre elles, c'est-à-dire toutes les instructions qui ont le même N° de lien (dans cet exemple, considérer les trois instructions A3, A4 et A5 comme étant liées).

(2) considérer les types logiques de liens (dans cet exemple, les trois instructions A4, A5 et A6 sont liées par des ET logiques)

10 (3) vérifier si A4 est vérifiée (dans cet exemple, vérifier si l'opérateur qui envoie l'instruction A4 est autorisé - la réponse est OUI du fait que l'instruction A1 est vérifiée)

15 (4) si OUI, vérifier si A5 est vérifiée (dans cet exemple vérifier si la carte a les droits pour l'abonnement diffusé - la réponse est OUI du fait que l'instruction A2 est vérifiée, c'est-à-dire que l'abonnement diffusé ABT1 est égal à l'abonnement acquis ABT1)

20 (5) si OUI, vérifier si A6 est vérifiée (dans cet exemple vérifier si la carte a les droits pour le niveau diffusé - la réponse est OUI du fait que l'instruction A2 est vérifiée, c'est-à-dire que le niveau de l'émission diffusée (niveau 2) pour l'abonnement ABT1 est inférieur ou égal au niveau acquis dans la carte (niveau 3) pour ce même abonnement ABT1)

25 (6) si OUI, vérifier si la date courante est comprise entre les dates de début et de fin pour l'abonnement diffusé (dans cet exemple la réponse est OUI si la date courante est comprise entre D1 et F8 qui sont les dates de début et de fin pour ce même abonnement ABT1)

30 (7) le programme spécifique P1 autorise alors le décodage par le décodeur 16 si il a obtenu :

 une réponse OUI pour l'instruction A4
 ET une réponse OUI pour l'instruction A5
 ET une réponse OUI pour l'instruction A6
 ET une réponse OUI pour l'étape (7) qui est une
35 étape spécifique du programme P1 (c'est-à-dire un contrôle qui

concerne spécifiquement le programme P1 qui sert à vérifier les conditions obligatoires pour autoriser le décodage).

Autrement dit, le programme spécifique vérifie l'existence des liens logiques entre les instructions qui arrivent
5 (dans cet exemple le programme spécifique P1 vérifie les instructions de proposition de décodage, c'est-à-dire les instructions A4, A5 et A6, à partir des droits qui sont acquis dans la carte, c'est-à-dire des droits définis par les instructions antérieurement stockées A1, A2 et A3). Le
10 programme peut aussi effectuer des vérifications complémentaires qui sont spécifiques à la fonction que le programme implémente. (dans cet exemple, le programme P1 effectue la vérification spécifique de l'étape (7)).

15 On voit que dans la zone mémoire Z2 de la carte à mémoire 10, on peut stocker à la suite les différentes instructions qui arrivent A1, A2, etc ..., sans que l'ordre de stockage n'ait d'importance. Si une instruction est supprimée, les instructions qui suivent peuvent être décalées pour
20 supprimer l'espace mémoire libéré, ceci dans le cas où toutes les instructions n'ont pas la même longueur. Si le formatage des instructions est tel que les instructions ont toutes la même longueur, on ne décale pas les instructions qui suivent une instruction supprimée parce que l'on peut stocker une nouvelle
25 instruction dans l'espace mémoire libéré.

En fait, quand un programme spécifique est exécuté, l'opération qui consiste à vérifier tous les liens entre les différentes instructions stockées est une opération qui est effectuée en passant en revue successivement toutes les
30 instructions stockées. C'est pour cette raison que l'ordre de stockage des différentes instructions n'a pas d'importance

La figure 3 illustre une configuration générale d'une organisation de production et de diffusion de plusieurs chaînes
35 de télévision à péage. Cette configuration est donnée à titre

d'exemple dans le seul but de montrer les possibilités d'adaptation et d'évolution du système selon la présente invention. Comme cela est représenté sur cette figure, on suppose que, dans une région donnée, il existe plusieurs

5 producteurs de télévision P1, P2, P3. Le producteur P1 produit les chaînes C1, C2 et C3. Le producteur P2 produit la chaîne C4, le producteur P3 produit la chaîne C5. Il existe aussi plusieurs diffuseurs (par exemple un diffuseur assurant la diffusion à l'aide d'un réseau hertzien, un autre diffuseur assurant une

10 diffusion par câble, etc...). On trouve dans cet exemple trois diffuseurs différents, D1, D2, D3. Cette configuration générale doit être communiquée à l'ensemble des cartes à mémoire du système selon l'invention. Cette communication peut être effectuée par exemple en introduisant dans le signal vidéo (par

15 exemple lors du retour vertical) de toutes les chaînes émises les instructions qui décrivent cette configuration. Cette émission des instructions simultanément sur toutes les chaînes émises peut être répétée périodiquement, par exemple lors de chaque retour vertical du signal vidéo ou chaque seconde. Par

20 conséquent, à tout moment, lorsqu'une carte à mémoire est connectée à un décodeur d'abonné qui est en fonctionnement de façon à recevoir l'une des chaînes émises, ces instructions de description de la configuration générale sont automatiquement stockées dans la carte à mémoire. Ces instructions de

25 description de configuration sont les suivantes :

$$P1 = C1 + C2 + C3$$

$$P2 = C4$$

$$P3 = C5$$

$$D1 = P1 + P2 + P3$$

30 $D2 = P1 + P2$

$$D3 = P1 + P3$$

La signification de ces instructions écrites ici de façon symbolique est la suivante : le producteur 1 peut produire les

35 chaînes 1, 2 et 3, le producteur 2 peut produire la chaîne 4, le

producteur 3 peut produire la chaîne 5, le diffuseur 1 diffuse les émissions des producteurs 1, 2 et 3, le diffuseur 2 diffuse les émissions des producteurs 1 et 2, le diffuseur 3 diffuse les émissions des producteurs 1 et 3.

5 Si des modifications sont apportées à cette configuration générale, comme cela est vraisemblablement le cas au cours du temps, toutes les instructions contenues dans toutes les cartes à mémoire deviennent fausses. Cependant, comme on va le voir par la suite, la réactualisation, c'est-à-dire la mise à jour, des
10 instructions de configuration contenues dans toutes les cartes à mémoire est relativement facile à effectuer si on utilise un système selon la présente invention.

Par exemple, si la configuration générale est modifiée de telle sorte (comme cela est dessiné sur la figure 3 en pointillés)
15 que le producteur P2 produise en plus une chaîne C6 et que les diffuseurs D2 et D3 fusionnent pour ne former qu'un seul nouveau diffuseur D4 qui conserve physiquement l'ensemble des réseaux appartenant précédemment aux deux diffuseurs D2 et D3. On voit que cette modification de la configuration générale peut être
20 aisément prise en compte au niveau des cartes à mémoire. Pour cela, il suffit de rajouter deux nouvelles instructions :

$$P2 = C6$$

$$D4 = D2 + D3$$

Toutes les anciennes instructions restent valables. Les
25 nouvelles instructions rajoutent les liens logiques qui se présentent les modifications de la configuration.

En fait, cette modification de la configuration générale peut s'exprimer d'une façon logique, selon une algèbre booléenne, et cette description logique ou booléenne correspond à de
30 nouveaux liens qui viennent s'ajouter aux liens qui existaient déjà. On comprend que ce nouveau concept permette une très grande facilité de la gestion et de la communication des informations qui doivent être communiquées aux cartes à mémoire du système.

Si, après avoir mis à la disposition du public un premier lot de cartes à mémoire qui peut fonctionner avec la configuration générale qui vient d'être décrite, on veut diffuser un autre lot de cartes à mémoire qui présentent toutes une extension particulière par rapport aux possibilités de réception de chacune offertes par cette configuration générale, par exemple si ce nouveau lot de cartes à mémoire se caractérise par le fait qu'on veuille que ces cartes puissent débrouiller la chaîne du producteur P3 au travers du diffuseur D2 (ce qui n'est pas permis par le premier lot de cartes), il suffit de stocker initialement dans toutes les cartes du second lot l'instruction suivante :

D2 = P3

On pourrait trouver ainsi un grand nombre d'autres possibilités pour modifier à l'infini les caractéristiques commerciales du système selon l'invention.

La figure 4 représente la structure d'une carte à mémoire d'un système selon la présente invention. Cette carte à mémoire peut comporter un unique circuit intégré comprenant principalement une unité centrale de traitement (CPU) 22, une mémoire morte ROM 24, une mémoire vive RAM 26 et une mémoire morte électriquement effaçable EEPROM 28, un circuit d'entrée/sortie (I/O) 30 et un dispositif de communication de données reliant ces différents éléments 32. La mémoire ROM 24 contient des informations permanentes permettant de gérer les entrées/sorties, un programme de base du fonctionnement initial de la carte et un ou plusieurs programmes définissant les commandes et les instructions générales de la base de données. La mémoire morte électriquement effaçable 28 peut mémoriser l'ensemble des instructions de la base de données et éventuellement d'autres commandes de base de données que l'on peut vouloir effacer ainsi que les programmes spécifiques P1, P2, P3, etc... dont il a été fait état précédemment.

Les exemples qui viennent d'être donnés en relation avec les figure 2 à 4 ne sont donnés que dans le but de faire comprendre le concept de la présente invention et ne constituent pas une quelconque limitation de la portée de l'invention.

5

Les systèmes classiques permettent à un opérateur l'utilisation totale, partielle ou partagée de zones mémoires réservées selon des paramètres définis, en lui autorisant d'effectuer des opérations de lecture, écriture, de modification et/ou de calcul en fonction d'ordres donnés concernant certaines informations se trouvant dans une zone déterminée.

Le système selon l'invention prévoit de réaliser les opérations de lecture, d'écriture, de modification et/ou de calcul en fonction des liens trouvés, ce qui signifie que l'opérateur n'a pas accès à une zone définie mais à une information satisfaisant au lien demandé par l'opérateur.

Les conditions d'accès sont accordées en fonction de données liées, par définition, aux droits d'accès, qui peuvent être constitués par exemple par un mot de passe ou un algorithme de chiffrement.

Parallèlement à la faculté de moduler les droits d'accès ou d'utilisation de l'information, ce nouveau système permet d'optimiser l'utilisation de la ressource mémoire et de pouvoir s'accommoder de zones de mémoire devenues inutilisables.

L'accès à l'information est régi par des programmes P1, P2, P3, etc... écrits dans un langage de type "langage de base de données relationnelle". Ces programmes peuvent être pré-définis dans la carte à mémoire 10 sous forme compilée, peuvent être téléchargés sous forme compilée ou peuvent être téléchargés avec des macro-instructions à interpréter. Le concept de programme interprété permet de limiter les droits d'un opérateur.

Les applications bancaires prévoyant plusieurs prestataires pourront utiliser un concept de lien inter-opérateurs établi par échange de cryptogrammes. Dans ce cas, le

demandeur du lien enverra un cryptogramme d'identification muni d'un jeton (identification de transaction). Le récepteur vérifiera la validité du message et, en cas de succès, mémorisera le jeton. Ce concept permet de définir précisément
5 les relations inter-zones dans une carte à mémoire.

Le nouveau concept pourra être utilisé comme suit :

10 A. On considère que le système de gestion de l'opérateur et l'ensemble de toutes les cartes à mémoire forment une base de données relationnelle. Chaque opération effectuée entre le système de gestion de l'opérateur et une partition des cartes à mémoire peut être modélisée comme une commande de type "langage de gestion de base de données relationnelle".

15 B. Une même carte à mémoire peut faire partie de plusieurs bases de données relationnelles intégrant un système de gestion de l'opérateur et des cartes à mémoire, à savoir qu'elle peut faire partie de plusieurs entités.

20 C. Les commandes et demandes d'information provenant de l'extérieur déclenchent l'exécution d'un programme écrit dans un langage de type "langage de gestion de base de données relationnelle" permettant de définir de façon précise les droits d'accès à l'information et les traitements. Les programmes peuvent mémoriser sous forme compilée ou à interpréter.

25 D. Par cette structure, il est possible de réaliser un système où aucun élément du système ne contient toutes les informations. Pour que le système puisse fonctionner dans son ensemble, il est nécessaire de disposer des systèmes de gestion et des cartes à mémoire associées, ces dernières jouant le rôle
30 d'interface entre les différentes composantes du système.

E. La structure interne de la carte à mémoire est organisée en tant que base de données relationnelle. Elle permet de gérer de façon "dynamique" les droits ou autres informations mémorisées.

F. La structure de la base de données de chaque carte à mémoire associe des informations entre elles, ainsi qu'avec des programmes et des clés de chiffrement (sécurité de transmission). La notion de clé de chiffrement est en fin de
5 compte considérée comme un lien entre une information, la méthode de chiffrement et la clé de chiffrement.

G. La structure de la base de données permet de transmettre des informations entre le centre de gestion et la carte à mémoire de façon compacte en envoyant des
10 informations de modification de la base de données, plutôt que d'envoyer directement celle-ci pour créer une copie. La structure de lien permet de vérifier que toutes les informations ont été reçues avant de les rendre utilisables.

H. La mise en place de ce nouveau système exploite la
15 technologie actuelle des cartes à mémoire, à savoir que la taille mémoire "inscriptible" est relativement faible. L'établissement des liens ou leur vérification se fait par un examen complet de la mémoire. La mémoire stocke simplement toutes les informations les unes à la suite des autres, avec les
20 informations de lien intégrées. Par contre, ce système n'autorise jamais une lecture "directe" d'une zone mémoire, seule la lecture par lien interposé est possible, pour autant que l'accès soit autorisé.

I. La distinction entre les informations sujettes à
25 autorisations différentes se fait par un lien avec un algorithme de chiffrement et une clé de chiffrement ou un mot de passe et non par un contrôle d'accès déterminé par une procédure d'authentification permettant l'accès à l'information dans une zone sélectionnée.

J. La structure de la mémoire ne prévoit pas de lieu de
30 stockage prédéfini pour chaque fonction, à savoir l'information, les programmes, les clés de chiffrement et les dates de validité. Par contre, elle dispose d'un espace continu où les informations sont stockées et où leur utilisation est régie par des liens entre
35 elles (conditions). On peut modéliser cette structure en

considérant que la mémoire est remplie de données pouvant être une date, une clé, un crédit, un logiciel et/ou des données générales et un lien définissant les conditions d'utilisation.

5 K. Le système présenté dispose d'un système de "nettoyage" des zones non-utilisées. Le nettoyage est rendu possible par un lien "date limite de validité" qui permet d'éliminer automatiquement les données ou liens caducs. Il est naturellement également possible de libérer explicitement par ordre des zones déterminées.

10 L. La notion de porte-monnaie est définie comme un système où l'établissement d'un lien est "payant". Cependant, seuls les établissements de liens "autorisés" peuvent avoir lieu et débitent le crédit.

15 M. De nouvelles fonctionnalités peuvent être téléchargées sous la forme de processus pouvant être appliqués à des données liées. Par cette méthode, il sera possible de limiter l'utilisation de ces nouvelles fonctionnalités à des opérations sélectionnées.

20 N. Les commandes d'établissement de lien peuvent être réalisées, soit en adressant directement une carte à mémoire, soit en considérant que celle-ci appartient à un groupe où chaque carte est adressée par un code hiérarchisé (appelé bit map). La notion d'adresse peut également être considérée comme un lien.

25 O. Les cartes à mémoire peuvent également recevoir des commandes demandant une fonction spécifique (de cryptage par exemple). Dans un tel cas, la fonction à appliquer peut être définie par un lien vers une telle fonction.

P. L'ensemble des commandes que peut exécuter une carte à mémoire peut être crypté.

30 Q. Les échanges d'information inter-zones peuvent se faire de façon cryptée et avec jetons, pour permettre une sécurité inter-zones, principalement destinée aux applications bancaires.

L'intérêt du nouveau concept selon l'invention est le suivant.

Par opposition au système de carte à mémoire de deuxième génération, le système décrit ici permet de moduler
5 les droits d'accès à l'information de façon plus fine que celle qui consiste à définir à chaque "opérateur" un droit d'accès. Le système proposé permet de définir des droits d'accès pour chaque information définie.

Ce système permet de faire jouer à une carte à mémoire
10 un rôle central dans la gestion de l'information, en se trouvant au coeur d'un système, plutôt que de la considérer comme étant une juxtaposition de copies de données existantes dans un système de gestion.

Les systèmes classiques prévoient que l'information soit
15 établie par un opérateur de façon complète avant d'être transférée à la carte à mémoire. Cela signifie qu'il est nécessaire de concentrer l'ensemble des informations propres à un opérateur avant de les transférer à la carte à mémoire (même s'il n'est pas nécessaire d'effectuer cette opération au même
20 endroit pour tous les opérateurs d'une même carte).

Le système proposé permet d'établir l'information à l'intérieur de chaque carte à mémoire. Cet établissement "à l'intérieur" permet d'exploiter de façon optimale la notion de "secret partagé", ne nécessitant pas de construire une image du
25 contenu de la carte à mémoire avant de le transférer.

Ce concept signifie que, pour un opérateur donné, l'information est distribuée entre son système de gestion et l'ensemble des cartes, car il n'a pas d'accès autre par par les cartes à mémoire à certains liens.

30 En pratique, la structure d'information définie permet de composer l'information à l'intérieur de la carte plutôt que de transmettre à la carte à mémoire des informations toutes prêtes.

La motivation originale provient des limites des
35 possibilités de la carte à mémoire dans les utilisations en

télévision à péage. L'introduction de la notion de base de données sur une carte à mémoire a été nécessaire pour les raisons suivantes :

5 A. Notion de grappe

Statistiquement, l'évolution du contenu des cartes se fait à 95% de façon implicite (reconduction simple des droits de la carte) et à 5% de façon singulière. Selon les systèmes classiques l'ensemble des opérations (reconduction et traitement
10 singuliers) se fait de façon similaire en transmettant le nouveau contenu de la carte à mémoire (ou de la zone concernée). Cette méthode est la seule pratiquement utilisable dans le concept classique ; il est en effet dangereux de donner 100% de droits illimités à des cartes et de détruire les droits concernant 5%
15 des cartes pour y réintroduire les nouveaux droits, car il est impossible de garantir que les informations de destruction soient bien arrivées.

La solution proposée ici permet de lier par exemple l'ensemble des informations à une date de validité qui sera la
20 seule à être reconduite, ceci permet de prolonger la validité des informations en envoyant une seule information plutôt que de traiter ses composantes. Pour les 5% à traiter de façon singulière, il sera nécessaire de reconstruire de nouveaux liens.

25 B. Autorisations multiples

Selon l'approche classique en télévision à péage, l'opérateur du service gère le parc d'abonnés comme une seule entité homogène. Toute prise d'abonnement ou modification de ce dernier ne pourra se faire que par l'opérateur directement. Selon
30 cette logique il y aura autant de zones opérateur sur la carte que d'opérateurs fournissant un service. Dans cette logique, seul l'opérateur "original" pourra "couper le robinet" à un client ne payant pas. A titre d'exemple, on peut considérer un client X abonné à la chaîne A au travers d'un réseau câblé R ; si le client
35 X ne paie pas au réseau câblé sa redevance "câble", le réseau R

devra demander à la chaîne A de suspendre les droits dont il dispose. Cet état de fait alourdit de façon considérable la gestion en augmentant le volume d'informations échangées, notamment entre le réseau R et la chaîne A, ainsi qu'entre la chaîne A et l'abonné X. En outre, cela demande que les périodes de paiement entre la chaîne A et le réseau R soient compatibles et que le réseau R communique la liste des mauvais payeurs.

Toutefois, dans la logique des systèmes classiques, il est possible que la chaîne A délègue complètement la gestion de ses abonnés (sur le réseau R) au réseau R. Cette solution présente l'inconvénient de demander à la chaîne A de faire totalement confiance au réseau R sur le plan commercial. A défaut de cette solution, le réseau R pourra toujours déléguer un technicien pour sceller la prise de l'abonné...

Le système proposé permet de résoudre de façon élégante ce cas en liant la possibilité de recevoir la chaîne A chez l'abonné X à une information "accord" du réseau R. Par ce principe, le réseau R peut autoriser ou non l'accès à A, sans avoir à demander à la chaîne d'agir. En outre, la durée des autorisations pourra être différente.

La mise en oeuvre de cette solution demandera à la chaîne A de créer un abonnement d'une durée définie et soumis à une condition qui sera accordée par le réseau R.

La création de tels liens pourra être variable selon les clients, permettant de moduler le schéma d'autorisation des clients en fonction de la distribution du signal. De cette façon, un client Y pourra être abonné par le signal original de la chaîne A, alors que le client X passera par le réseau R.

30 C. Durée du contrat et paiement

Selon la définition classique des abonnements, la période contractuelle correspond à la période de paiement, à savoir que pour un abonnement d'une année, le paiement sera annuel.

Pour faciliter la prise d'abonnement, certaines entreprises ont fait intervenir la possibilité d'effectuer un paiement fractionné.

5 En télévision à péage cela pose un problème lorsque la durée du contrat est d'une année, alors que le paiement est mensuel. En effet, si l'on confère un droit d'une année et que le client ne paie pas après un mois, il sera nécessaire de supprimer le droit sur la carte à mémoire. Toutefois, il n'est pas possible d'être certain que la carte ait bien reçu le message de
10 suppression et il faudra le répéter fréquemment durant toute la durée du contrat. La parade à ce problème consiste à donner des droits plus courts (2 mois) et de les prolonger régulièrement ; cependant, cette solution présente l'inconvénient de ne pas refléter la réalité du contrat(ce qui sera visible lors de la
15 consultation des droits).

Le système proposé permet quant à lui de considérer un contrat annuel avec, pour être valable, une condition qui est que le paiement soit réalisé. On disposera d'un contrat valable un an et d'autorisation "d'utilisation" mensuelle correspondant au
20 paiement mensuel. Cette solution correspond d'ailleurs à la définition contractuelle précise.

D. Distributions multiples

La vision classique des systèmes de télévision à péage
25 prévoit que chaque "opérateur" dispose d'un accès direct à une zone réservée chez chaque abonné. Cette vision oblige l'opérateur à gérer lui-même chaque abonné.

Le système proposé permet à un opérateur de déléguer la fonction de gestion d'un sous-ensemble d'abonnés. Cela signifie
30 qu'une chaîne A peut déléguer la gestion d'une partition P1 de cartes pour les abonnés au réseau R1 (à condition d'avoir les coordonnées "carte à mémoire" des abonnés) et de déléguer la gestion de la partition P2 à un réseau R2.

Dans ce cas, les réseaux R1 et R2 géreront de façon
35 indépendante les abonnés à la chaîne A. En outre, ils auront la

possibilité d'inclure la chaîne A dans un "package" de chaîne, et ceci de façon indépendante entre R1 et R2. Par cette délégation, il est possible à la chaîne A d'offrir un "ensemble" de N abonnements qui seront gérés, facturation comprise, par un
5 sous-opérateur.

Le système permet également à une chaîne A de gérer l'ensemble de ses abonnés alors que la fonction de codage des émissions est déléguée à une ou plusieurs autres entreprises.

10 E Structure auto-porteuse

Selon le modèle classique, l'opérateur détient l'ensemble des secrets correspondant à chaque carte à mémoire. L'envoi de messages entre l'émission et une carte à mémoire se fait en indiquant les références des clés cryptologiques à utiliser,
15 typiquement le numéro de clé de gestion ou de clé de service. Ce concept est bien répandu dans les systèmes avec communication point à point, cependant il devient difficile à gérer lorsque l'architecture devient plus complexe.

Le système proposé fait appel à la notion de clés
20 rattachées à un type d'information sur une période de temps, à savoir que les informations relatives à un certain lien seront communiquées durant une période donnée en utilisant une certaine clé. Il est également possible d'avoir plusieurs clés simultanément valables.

25 Ce concept permet de ne pas nécessiter l'envoi de la référence de la clé utilisée lors d'une transaction, en simplifiant la gestion. Le système de cryptage, qui pourra être décentralisé ne devra connaître que la clé de cryptage pour envoyer les informations, sans avoir à indiquer les références.

30

F. Fonction "Banque"

Les systèmes classiques prévoient une gestion de crédit propre à chaque opérateur. Le crédit est alimenté par chaque opérateur et est utilisable exclusivement pour des débits
35 relatifs à cet opérateur (par l'abonné).

Le système proposé permet de créer une notion d'opérateur "banque" qui peut gérer un crédit commun à un certain nombre d'opérateurs et qui peut être rattaché à certains liens.

- 5 La fonction banque fera payer l'établissement d'un lien ; en échange, elle autorisera son utilisation.

EXEMPLES COMPARATIFS DANS LE DOMAINE DE LA TELEVISION A PEAGE - CONTRAT MULTI-CHAINE

10

Système classique :

- Traditionnellement, un contrat d'abonnement multi-canaux est traité par la tenue à jour de droits indépendants pour chaque canal. Si X est abonné aux canaux A, B et C, la carte à
15 mémoire de son décodeur recevra indépendamment les droits d'accès aux canaux A, B et C pour une durée limitée, correspondant en principe à la durée de paiement. A la réception de chaque paiement, l'opérateur enverra de nouveaux droits correspondant à la période payée. Selon cette méthode, la carte
20 de l'abonné recevra autant de messages qu'elle a d'abonnements, plus des messages relatifs aux clés de cryptage à utiliser.

En cas de non paiement, les droits ne seront pas reconduits à l'échéance suivante et/ou les ordres d'annulation seront envoyés.

- 25 En cas de non reconduction du contrat, les droits ne seront pas renouvelés.

En cas d'adjonction d'un canal au contrat, il faudra gérer les droits correspondants à chaque échéance (une commande de plus).

30

Système selon l'invention :

L'opérateur responsable de la diffusion des trois canaux créera un noyau contrat de base, lié à l'opérateur (pour définir la paternité), à un descripteur des trois canaux choisis, à la durée

du contrat et à une variable paiement qui sera gérée par un opérateur responsable de l'encaissement des abonnements.

5 A chaque paiement, l'opérateur responsable de l'encaissement étendra la validité du lien de la période ainsi couverte.

Lors de chaque reconduction du contrat, l'opérateur responsable de la diffusion reconduira simplement la validité du lien "durée du contrat".

10 En cas de non-paiement, l'opérateur responsable de l'encaissement ne renouvellera pas le lien de paiement et/ou le détruira.

En cas de non-renouvellement du contrat, l'opérateur responsable de la diffusion ne renouvellera pas la durée du contrat.

15 En cas d'adjonction d'un nouveau canal au contrat, il suffira d'ajouter le nouveau canal avec un lien vers le contrat précédent, puis tout sera implicite lors des opérations subséquentes.

20 La principale différence entre les deux conceptions provient de la différence entre le cas classique du système de gestion (l'opérateur doit créer une image de la carte à mémoire pour la transférer intégralement) et le concept S-RDB qui permet de n'envoyer que des modifications. En outre, si dans le modèle classique le centre de gestion de l'opérateur contrôle
25 simultanément le contrat et le paiement, dans le second cas ces deux fonctions peuvent être traitées par deux centres distincts.

EXEMPLES COMPARATIFS DANS LE DOMAINE DE LA CARTE BANCAIRE - CONCEPT DE CREDIT

30 Système classique :

Le concept classique considère qu'une carte à mémoire bancaire est "mono-opérateur", ce qui signifie que la carte possède une identité liée qu'à un seul organisme. La notion de mot de passe ou d'algorithme de chiffrement est directement

rattachée à cet opérateur, ce qui signifie que l'opérateur a une visibilité sur le mot de passe du porteur de carte.

L'utilisation d'une telle carte se complique lorsqu'il est nécessaire de permettre l'emploi de la carte sur des systèmes ne dépendant pas de l'opérateur. Dans un tel cas, l'opérateur devra
5 soit dévoiler ses secrets à d'autres opérateurs, soit établir une connexion en temps réel avec eux.

Alternativement, il sera possible de créer une zone réservée à chaque opérateur, cependant une telle structure ne
10 permet pas de bloquer le compte en cas de dépassement de la limite de crédit.

Nous aurons donc dans tous les cas un système lourd et contraignant.

15 Système selon l'invention :

En admettant que le détenteur de carte X possède un compte à la banque A et désire pouvoir retirer de l'argent aux banques B et C et de disposer d'un concept carte de crédit du pool P, l'émetteur va générer les zones opérateur suivantes sur la
20 carte à mémoire :

X : Zone du porteur

A : Zone de la banque gérant le compte

B : Zone de la banque B

25 C : Zone de la banque C

P : Zone du pool P

La zone X contiendra un lien conditionnel qui s'établira contre la présentation du mot de passe du porteur. Le lien ne
30 pourra être considéré comme valable que si le mot de passe correct est introduit.

La zone A contiendra l'état du compte et un lien vers la zone X pour demander le mot de passe, un lien conditionnel vers les zones B, c et P, un lien pour la fonction débit de crédit du
35 compte A et une liaison vers les fonctions de cryptage entre (A

et B), (A et C) et (A et P). L'établissement de ces liens se fera contre un échange de cryptogrammes validés par les fonctions de cryptage.

5 Le zones B, C et P contiendront un lien conditionnel avec la zone A, un lien avec les fonctions de cryptage vers A, un lien avec la fonction de cryptage vers le monde extérieur et un lien définissant une demande de débit. L'établissement de ces liens se fera contre un échange de cryptogrammes validés par les fonctions de cryptage.

10

L'échange-type se fera comme suit :

1. Le porteur introduit sa carte dans le lecteur de l'opérateur P.

15 2. L'opérateur identifie la zone P par un échange de cryptogramme et demande un lien avec la fonction débit de crédit D.

20 3. La zone P établit le lien avec l'opérateur externe, mais définit que pour que le lien soit valable, il doit être complété par un lien vers la zone A.

4. La zone A reçoit la demande de lien de P, mais définit que ce lien nécessite un lien vers la zone X et un lien "débit de crédit".

25 5. La zone X reçoit la demande de lien de A mais nécessite que le mot de passe soit présenté. La zone X demandera au lecteur de présenter le mot de passe.

6. Si le mot de passe correct est présenté, la zone X accordera le lien avec la zone A.

30 7. La zone A pourra alors établir un lien conditionnel avec la zone P, sous réserve de débit.

8. La zone P pourra alors fermer le lien avec l'opérateur externe.

9. La fonction demande de débit pourra être exécutée en échange du débit de crédit, de la zone A.

10. La fonction de débit fournira un cryptogramme d'autorisation vers la zone P.

11. La zone P fournira un cryptogramme d'autorisation vers l'opérateur externe.

5 12. L'opérateur externe fournira un cryptogramme de quittance vers la zone P.

13. La zone P fournira un cryptogramme de quittance à la zone A.

10 14. La zone A fournira un cryptogramme de quittance à la zone X.

L'ensemble des opérations réalisées entre les zones se fait de façon cryptée afin de garantir l'authenticité des intervenants.

15 Par ce concept, il est possible d'avoir des échanges d'informations à l'intérieur de la carte à mémoire selon une logique prédéfinie et entre parties ayant des rapports contractuels.

20 Il ne sera pas possible à l'opérateur d'une zone de connaître les secrets d'un autre opérateur, car tous les échanges d'informations se feront en fonction des liens prédéfinis et couverts par des échanges "cryptés".

25 EXEMPLES COMPARATIFS DANS LE DOMAINE DU DECRYPTAGE SOUS CONDITION

Les systèmes de contrôle d'accès demandent à effectuer le décryptage d'une information en fonction de critères d'accès qui autorisent un tel décryptage.

30 Système classique :

Les solutions classiques prévoient qu'une carte à mémoire délivre le résultat d'un décryptage si un opérateur envoie un message crypté et que des conditions d'accès soient remplies. Les conditions d'accès sont définies au départ, par exemple
35 droits d'accès avec limite de date, numéro de référence et clé de

décryptage valide. Si ces conditions sont remplies, la carte à mémoire pourra délivrer l'information décryptée. Ce schéma prévoit que les informations soient mémorisées dans des cases spécialisées pour chaque type d'information. Cette solution
5 présente la limitation de ne fonctionner que dans la limite de la zone réservée à un opérateur et de ne pas permettre de redéfinir après coup de nouvelles conditions d'accès.

Système selon l'invention :

10 La solution S-RDB fonctionne selon un concept où les conditions sont définies sous forme d'un programme écrit dans un langage de type SQL. Cela signifie que les conditions d'accès pourront être modulées à loisir, en faisant intervenir au besoin des données résidentes chez d'autres opérateurs.

15 La délivrance d'une information décryptée ne pourra avoir lieu que si le programme réussit tous les tests nécessaires, tels que définis. Il est également possible de définir plusieurs chemins qui pourront aboutir à la délivrance de l'information.

Usuellement, le programme qui traitera l'information sera
20 compilé et ne pourra pas être modifié. Cependant, pour permettre des modifications subséquentes, il sera possible de télécharger un nouveau programme compilé (par un organisme suprême) et/ou d'autoriser un opérateur à télécharger un programme "à interpréter" lui permettant de définir un nouveau schéma
25 d'accès.

REVENDICATIONS

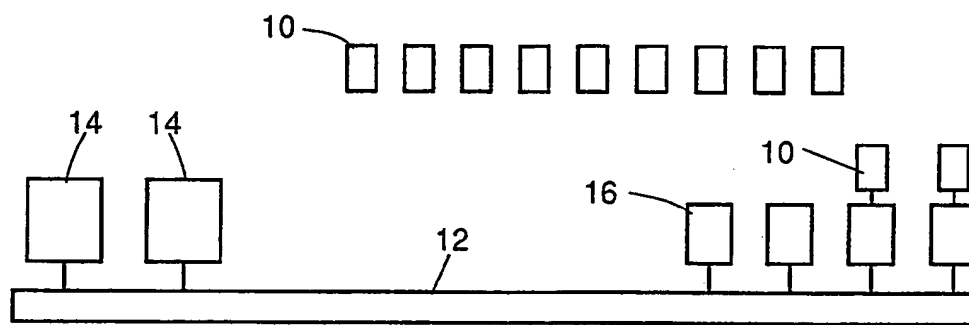
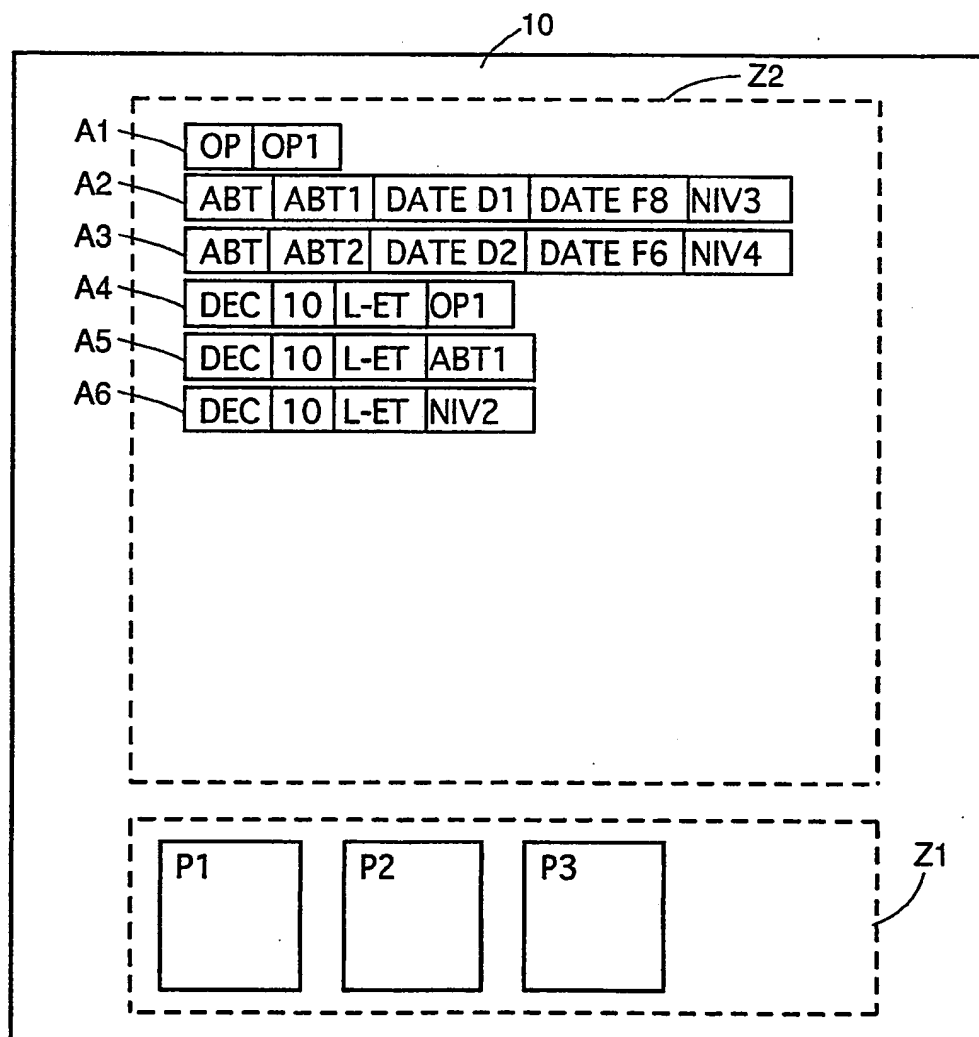
1. Système de traitement d'information comprenant un ensemble de cartes à mémoire et au moins une unité centrale de gestion, caractérisé en ce que les cartes à mémoire et l'unité centrale de gestion constituent ensemble une base de données relationnelle.

2. Système de traitement d'information selon la revendication 1, caractérisé en ce que chaque carte à mémoire contient une mémoire destinée à stocker un ensemble d'instructions (A1, A2,... , An), chaque instruction contenant un lien logique avec au moins une autre instruction.

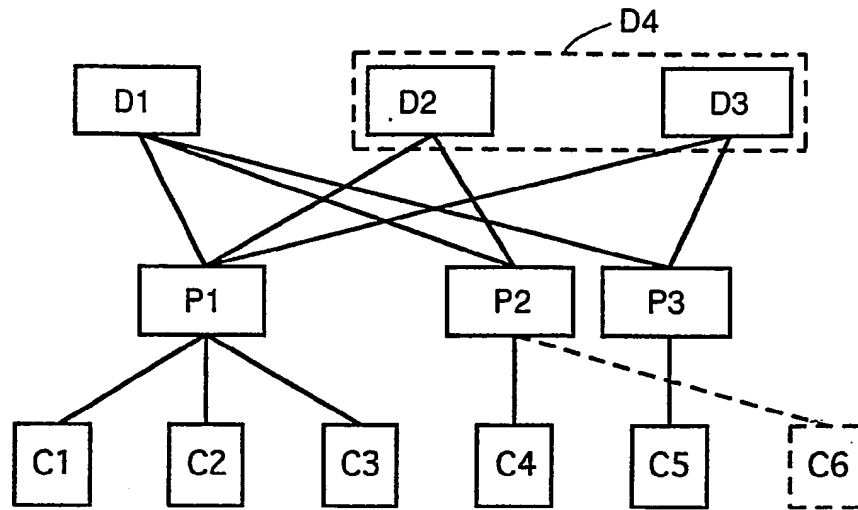
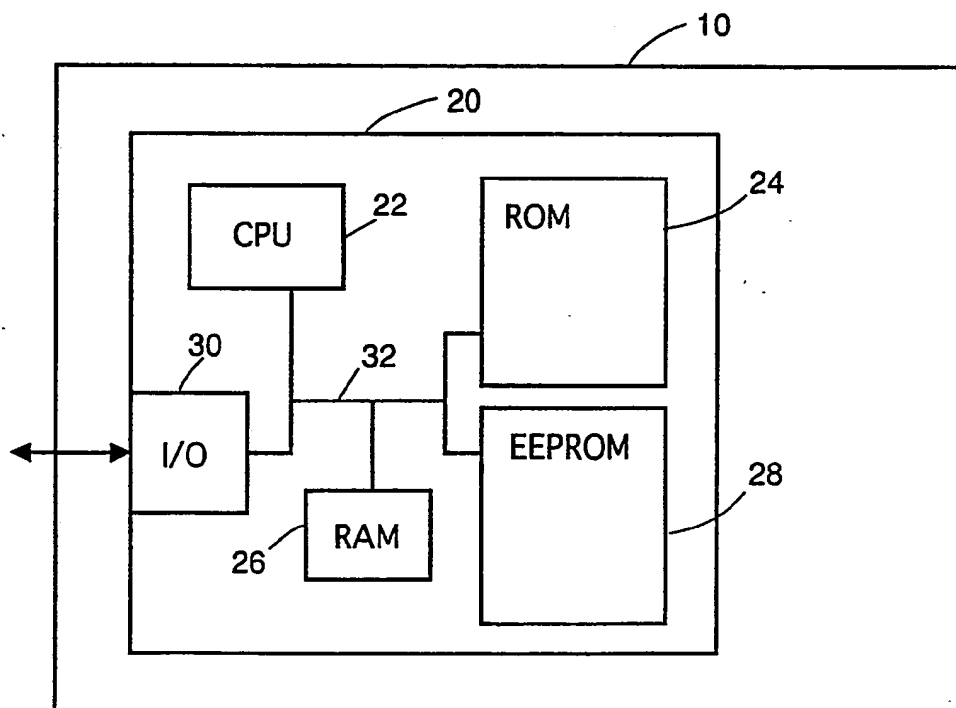
3. Système de traitement d'information selon la revendication 2, caractérisé en ce que chaque carte à mémoire contient en outre au moins un programme spécifique (P1) qui est destiné à exécuter une fonction spécifique de la carte à mémoire en appliquant les liens logiques qui sont instaurés entre les différentes instructions contenues dans la carte à mémoire.

4. Ensemble de cartes à mémoire, caractérisée en ce que chaque carte à mémoire de l'ensemble comprend des informations d'une base de données relationnelle et en ce que l'ensemble des informations dudit ensemble de cartes à mémoire constitue une mémoire de stockage d'une base de données relationnelle.

1/2

*Fig. 1**Fig. 2*

2/2

*Fig. 3**Fig. 4*

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLERAPPORT DE RECHERCHE
établi sur la base des dernières revendications
déposées avant le commencement de la rechercheFR 9212322
FA 477677

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
X	EP-A-0 361 491 (DEUTSCHE BUNDESPOST) * le document en entier * -----	1-4
		DOMAINES TECHNIQUES RECHERCHES (Int. Cl.5)
		G07F
Date d'achèvement de la recherche 23 JUIN 1993		Examineur TACCOEN J-F.P.L.
CATEGORIE DES DOCUMENTS CITES X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : pertinent à l'encontre d'un moins une revendication ou arrière-plan technologique général O : divulgation non-écrite P : document intercalaire T : théorie ou principe à la base de l'invention E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure. D : cité dans la demande L : cité pour d'autres raisons ----- & : membre de la même famille, document correspondant		

EPO FORM 1503 (3.92) (P0412)